PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-326630
(43)Date of publication of application : 22.11.2001

(51)Int.Cl. H04L 9/08
H04J 13/00

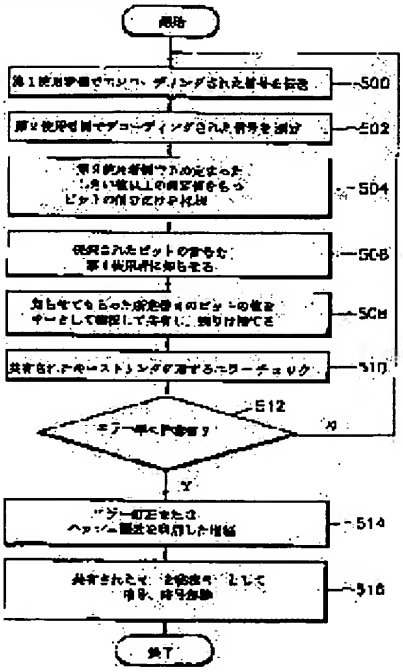
(21)Application number : 2001-088416
(22)Date of filing : 26.03.2001

(71)Applicant : SAMSUNG ELECTRONICS CO LTD
(72)Inventor : KIN GASEI

(30)Priority
Priority number : 2000 200015035 Priority date : 24.03.2000 Priority country : KR

(54) KEY AGREEMENT METHOD FOR SECURE COMMUNICATION SYSTEM IN MULTIPLEX ACCESS SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a key agreement method, with respect to encryption by common share of a secret key and, especially for a secured communication system in a multiplex access system.
SOLUTION: The key agreement method includes a step (step 500), where a 1st user device encodes a signal from a signal source by a bit sequence and transmits the encoded signal, a step (step 502) where a 2nd user device being a regular communication opposite party of the 1st user device decodes the signal transmitted from the 1st user device to measure the decoded signal, a step (step 504) the 2nd user device selects only bits, having a measured value that is a predetermined threshold value or over, a step (step 506), where the 2nd user device informs the 1st user device about only a number denoting to which order number bit in the bit sequence the adopted bit corresponds in place of the adopted bit value, and a step (step 508), where the 1st user device and the 2nd user device commonly share the adopted bit as a key string and abort the remaining it.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2001－326630
（P2001－326630A）
(43)公開日　平成13年11月22日(2001.11.22)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ	9/00	６０１Ｃ
Ｈ０４Ｊ　13/00		Ｈ０４Ｊ	13/00	Ａ
		Ｈ０４Ｌ	9/00	６０１Ｅ

審査請求　未請求　請求項の数５　ＯＬ　（全 10 頁）

(21)出願番号　特願2001－88416(P2001－88416)

(22)出願日　平成13年３月26日(2001.3.26)

(31)優先権主張番号　００－１５０３５

(32)優先日　平成12年３月24日(2000.3.24)

(33)優先権主張国　韓国（ＫＲ）

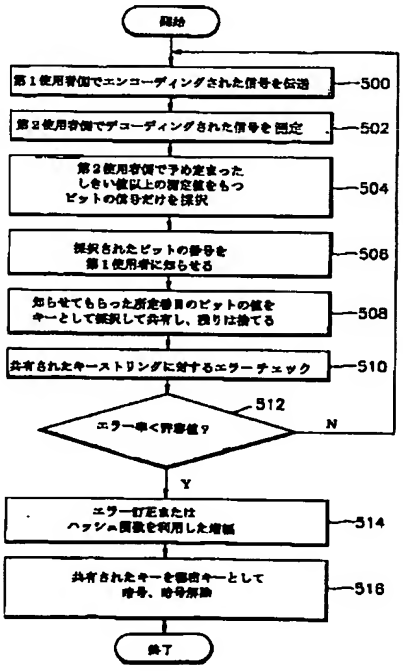
(71)出願人　390019839
三星電子株式会社
大韓民国京畿道水原市八達区梅灘洞416

(72)発明者　金　娥　正
大韓民国　ソウル特別市　瑞草区　蚕院洞　60－７番地　緑園アパート　101棟　804号

(74)代理人　100064414
弁理士　磯野　道造

(54)【発明の名称】　多重アクセス方式におけるセキュア通信システムのためのキー同意方法

(57)【要約】
【課題】　多重アクセス方式におけるセキュア通信システムのためのキー同意方法を提供する。
【解決手段】　第１使用者装置で、信号ソースからの信号をビットシーケンスでエンコーディングして伝送する段階（ステップ５００）と、第１使用者装置の正規の通信相手である第２使用者装置で、第１使用者装置から伝送された信号をデコーディングし、デコーディングされた信号を測定する段階（ステップ５０２）と、第２使用者装置が、予め定められたしきい値以上の測定値をもつビットだけを採択する段階（ステップ５０４）と、第２使用者装置が、採択されたビットの値の代わりに、採択されたビットがビットシーケンスの何番目のビットであるか、その番号だけを第１使用者装置に通知する段階（ステップ５０６）と、第１使用者装置及び第２使用者装置において、採択されたビットをキーストリングとして共有して、残りのビットを捨てる段階（ステップ５０８）とを含むキー同意方法とした。



【特許請求の範囲】

【請求項１】　多重アクセス方式におけるセキュア通信システムのためのキー同意方法において、（ａ）第１使用者装置で、信号ソースからの信号をビットシーケンスでエンコーディングして伝送する段階と、（ｂ）前記第１使用者装置の正規の通信相手である第２使用者装置で、前記第１使用者装置から伝送された信号をデコーディングし、デコーディングされた信号を測定する段階と、（ｃ）前記第２使用者装置が、予め定められたしきい値以上の測定値をもつビットだけを採択する段階と、（ｄ）前記第２使用者装置が、採択されたビットの値の代わりに、採択されたビットが伝送された前記ビットシーケンスで何番目のビットであるか、その番号だけを前記第１使用者装置に通知する段階と、（ｅ）前記第１使用者装置及び前記第２使用者装置において、前記採択されたビットをキーストリングとして共有して、残りのビットを捨てる段階とを含むことを特徴とするキー同意方法。

【請求項２】　前記（ｅ）段階後に、（ｆ）前記第１使用者装置及び前記第２使用者装置において共有されたキーストリングのうち部分集合ビットを選んでエラーチェックを行う段階と、（ｇ）前記エラーチェックにおいてエラー率が許容値内に含まれる場合に、伝送の安全を考慮してキーストリングを得、エラー訂正過程を経て最適化されたキーストリングを取得する段階と、（ｈ）前記エラー率が前記許容値を超える場合に、前記（ｅ）段階で採択されたキーストリングを廃棄して前記（ａ）段階へ戻り、前記（ｇ）段階を満足するキーストリングを得るまで前記（ａ）段階ないし前記（ｆ）段階を行う段階をさらに含むことを特徴とする請求項１に記載のキー同意方法。

【請求項３】　前記（ａ）段階で伝送された信号は雑音に敏感な信号であることを特徴とする請求項１に記載のキー同意方法。

【請求項４】　前記第２使用者装置は、他の使用者装置から生じる相互変調雑音の影響を受ける受信装置を使用することを特徴とする請求項１に記載のキー同意方法。

【請求項５】　前記（ｃ）段階のしきい値は、前記第２使用者装置において、少なくとも伝送率、伝送誤り率及び安全の度合いを考慮して定められることを特徴とする請求項１または請求項４に記載のキー同意方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、秘密キーの共有による暗号化に係り、特に、多重アクセス方式におけるセキュア通信システムのためのキー同意方法に関する。

【０００２】

【従来の技術】最近、情報化社会の進展に伴って新しい情報通信サービスが急増し、伝送帯域幅の確保及び通信に対する安全性がますます重要視されるようになってきた。特に、電子商取引、電子金融取引及びネットワーク情報サービスのように、電子認証、署名、識別を必要とするシステムが拡大するにつれて、個人情報の保護を求めようとする要求が高くなり、その結果として、暗号化の重要性が一層高まりつつある。

【０００３】通常、暗号システムにおいて、データは、使用者の正否を問わず任意の使用者が入手可能なアルゴリズムによりエンコーディング及びデコーディングされる。従って、暗号システムの安全性は、正規の使用者だけが利用可能な秘密キーにより左右される。安全性が保障された暗号化のために、暗号化関数の入力として用いられる秘密キーの設置、保管及び管理が重要なポイントであると言える。

【０００４】従来の暗号化は、そのほとんどがソフトウェアで処理を行う範疇に留まっており、外部からの物理的な攻撃や、優れた性能をもつコンピュータを利用した逆暗号化キーの抽出及び盗聴に対する防御力が弱かった。

【０００５】また、従来の暗号通信において、安全性のある通信のためには、平文（ｐｌａｉｎ　ｔｅｘｔ）をスクランブルする暗号化関数の入力変数として秘密キーが必要である。秘密キーの伝達や同意を私的なチャンネルを用いて実行するに当たって、いかに物理的に堅牢なチャンネルであるとしても、盗聴など外部の攻撃に対して破壊されて露出される危険性がある。このとき、盗聴者や攻撃者は、盗聴したビットに対する測定結果としてキーを探知したり、或いは元の伝達キーを復元して再伝送することも可能である。したがって、攻撃が生じた時であっても、正規の使用者装置ではその内容が盗聴されていることが分からない。

【０００６】一方、公開されたキーを用いる共通キーシステムは、数学的計算の複雑性に基づいている。最近、計算の並列遂行、新しいアルゴリズムの具現などが可能となった結果、光コンピュータ、量子コンピュータに対する研究が活発になりつつある。これは、共通キーシステムの安全性に大きな刺激的な要素として作用している。

【０００７】例えば、アルゴリズムを利用した方式として、共通キー及びナップサック方式に関する発明（米国特許　４２，１８，５８２）やＲＳＡ（Ｒｉｖｅｓｔ，Ｓｈａｍｉｒ　ａｎｄ　Ａｄｌｅｍａｎ）に関する発明（米国特許　４，４０５，８２９）があり、これらは複雑な数学的計算を必要とする。

【０００８】また、数学的計算の複雑性に基づいてない暗号システムとして、量子暗号によるキーの伝達（米国特許　５，３０７，４１０、米国特許　５，５１５，４３８）が挙げられる。しかし、このような量子暗号システムは、遂行のために極めて弱いパワーのコヒーレント状態にある光の使用を前提としているため、実用システムには適用し難い。

【０００９】
【発明が解決しようとする課題】本発明は前記事情に鑑みて成されたものであり、その目的は、多重アクセス方式のセキュア通信システムにおいて、使用者の通信システムを変更することなくそのまま継続使用しつつ、安全性が確立されたキーの同意を物理的な階層で実現することにより、不正行為者の盗聴を簡単な方法により無くし、安全なキーの通信を保証して安全性を増大させる、多重アクセス方式におけるセキュア通信システムのためのキー同意方法を提供することを目的としている。
【００１０】
【課題を解決するための手段】前記目的を達成するために、その請求項１に係る発明は、（ａ）第１使用者装置で、信号ソースからの信号をビットシーケンスでエンコーディングして伝送する段階と、（ｂ）前記第１使用者装置の正規の通信相手である第２使用者装置で、前記第１使用者装置から伝送された信号をデコーディングし、デコーディングされた信号を測定する段階と、（ｃ）前記第２使用者装置が、予め定められたしきい値以上の測定値をもつビットだけを採択する段階と、（ｄ）前記第２使用者装置が、採択されたビットの値の代わりに、採択されたビットが伝送された前記ビットシーケンスで何番目のビットであるか、その番号だけを前記第１使用者装置に通知する段階と、（ｅ）前記第１使用者装置及び前記第２使用者装置において、前記採択されたビットをキーストリングとして共有して、残りのビットを捨てる段階とを含むキー同意方法である。
【００１１】また、その請求項２に係る発明は、請求項１に記載の多重アクセス方式におけるセキュア通信システムのためのキー同意方法において、前記（ｅ）段階後に、（ｆ）前記第１使用者装置及び前記第２使用者装置において共有されたキーストリングのうち部分集合ビットを選んでエラーチェックを行う段階と、（ｇ）前記エラーチェックにおいてエラー率が許容値内に含まれる場合に、伝送の安全を考慮してキーストリングを得、エラー訂正過程を経て最適化されたキーストリングを取得する段階と、（ｈ）前記エラー率が前記許容値を超える場合に、前記（ｅ）段階で採択されたキーストリングを廃棄して前記（ａ）段階へ戻り、前記（ｇ）段階を満足するキーストリングを得るまで前記（ａ）段階ないし前記（ｆ）段階を行う段階をさらに含むことを特徴とする。
【００１２】また、その請求項３に係る発明は、請求項１に記載の多重アクセス方式におけるセキュア通信システムのためのキー同意方法において、前記（ａ）段階で伝送された信号は雑音に敏感な信号であることを特徴とする。
【００１３】また、その請求項４に係る発明は、請求項１に記載の多重アクセス方式におけるセキュア通信システムのためのキー同意方法において、前記第２使用者装置は、他の使用者装置から生じる相互変調雑音の影響を受ける受信装置を使用することを特徴とする。
【００１４】また、その請求項５に係る発明は、請求項１または請求項４に記載の多重アクセス方式におけるセキュア通信システムのためのキー同意方法において、前記（ｃ）段階のしきい値は、前記第２使用者装置において、少なくとも伝送率、伝送誤り率及び安全の度合いを考慮して定められることを特徴とする。
【００１５】
【発明の実施の形態】以下、添付した図面に基づき、本発明による多重アクセス方式におけるセキュア通信システムのためのキー同意方法について説明する。先ず、暗号通信システムにおいて、秘密キーを共有する方法について簡略に述べる。
【００１６】一時的に安全性のある通信を行う有線通信装置、または情報保護方式が具備されてない無線通信装置との通信のために、使用者が使用者装置の開始時に予め取り決めされた特定のキーを入力すれば、送信側の使用者装置（送信装置）が安全モードに設定または解除される。そして、この特定のキーにより送信された信号を受信した使用者装置（受信装置）も、送信装置と同様に安全モードに設定または解除される。これにより、正常的な通信、さらには、盗聴などの不正行為に対して安全な通信が可能になる。このように、特定のキーを利用した安全モードの設定は、通信のセットアップがなされる前に通知する方法を用いるか、通信のセットアップがなされた後で通信中に安全モードの設定または解除がなされるようにできる。
【００１７】このとき、特定のキーによる安全モードの設定時に用いようとするブロック暗号の秘密キーを共に伝送したり、或いは秘密キーが分かる方法を共に伝送できる。送信装置の暗号化器及び受信装置の暗号解除器に用いられるブロック暗号は、同一のアルゴリズム及び同一の秘密キーを用いる。このために、遠方に離れている送信装置と受信装置との間で秘密キーを共有する方法が必要となる。
【００１８】秘密キーを共有する方法の一つは、送信装置が生成した秘密キーを安全モードの設定時に受信装置に伝送することである。すなわち、安全モードの設定時に、１フレームのビットを安全モードの設定を意味する特定のパターンで伝送した後に、次フレームのビットを秘密キーとするか、マスタキーで暗号化された秘密キーとして伝送する。マスタキーを用いる場合、送信装置及び受信装置は同一のマスタキーを共有し、このマスタキーは信頼性のある許可やキー条件付き捺印証書など、責任のある機関が保管する。
【００１９】秘密キーを共有するもう一つの方法は、送信装置及び受信装置の内部に同一の方法で格納されている秘密キーの集合のうち、いずれか一つの秘密キーを安全モードの設定時に指定することである。すなわち、１フレームの情報ビットのうちの一部を安全モードの設定

を意味する特定パターンで伝送して、残りのビットを密かに格納された秘密キーなどのインデックスとして用いることである。このとき、格納された秘密キーは無線通信の場合、装置業者が提供するキーと、使用者が直接的に入力するキーとで構成される。

【００２０】これに対し、本発明による方法では、別に設けられたチャンネルを通じて送信装置及び受信装置の両方が秘密キーだけを交換する。このとき、交換される秘密キーは使用者が直接的に入力して生成したり、或いは乱数発生機能を利用して生成したものを用いる。この方法により交換された秘密キーは、前記した２番目の方法を利用して安全モードの設定時に指定されて使用される。本発明による方法は、特別に物理的な安全措置が施されていないチャンネルを通じても、送信装置及び受信装置の両方が秘密キーを交換し共有できるので、一般の通信装置のための暗号通信システムを構築することが容易である。

【００２１】本発明による暗号通信システムにおけるキー同意方法は、従来の通信方式のうち符号分割多重アクセス（ＣＤＭＡ：Ｃｏｄｅ　Ｄｉｖｉｓｉｏｎ　Ｍｕｌｔｉｐｌｅｘｅｄ　Ａｃｃｅｓｓ）方式、波長分割多重アクセス（ＷＤＭＡ：Ｗａｖｅｌｅｎｇｔｈ　Ｄｉｖｉｓｉｏｎ　Ｍｕｌｔｉｐｌｅｘｅｄ　Ａｃｃｅｓｓ）方式など、多重アクセス方式を用いる近距離通信網（ＬＡＮ）や長距離通信網（ＷＡＮ）で、チャンネル相互間に生じる相互変調雑音や測定器の熱雑音を利用して、不正行為者が正規の使用者と互いに相関しない測定結果を得るようにすることで、正規の使用者同士間において同意された秘密キーを正確に予測できないようにするだけでなく、不正行為者が伝送されるビットを棄損／再伝送して生じた汚染度を測定することにより、盗聴の発生可否及びその度合いが推測できるようにする。

【００２２】図１は、本発明が適用される一般的な通信システムにおける通信チャンネルの構造を説明するためのブロック図である。図１において、通信システムは、秘密キーを生成する送信側である第１使用者装置のエンコーダ（または変調器）１０２、マルチプレクサ１０４、伝送媒体１１０、受信側である第２使用者装置のデマルチプレクサ１２０、デコーダ（または復調器）１２２、検出器１２４などを含む。

【００２３】図１に示された通信システムでは、物理的な階層を用いて秘密キーを交換する。秘密キーを生成する第１使用者装置送信装置では、信号ソース１００で発生した信号をエンコーダ（または変調器）１０２によって、他の正規使用者が使用する各使用者装置に対して独立的に任意の信号に変調して伝送する。このとき、正規の使用者装置の各々に対して伝送される各信号は、マルチプレクサ（またはカップラ）１０４によって同一の伝送媒体１１０を共用して伝送される。

【００２４】伝送された信号は受信側である第２使用者装置でデマルチプレクサ（またはスリッタ）１２０によって分離され、該当デコーダ（または復調器）１２２を通過してフィルタリングされて、チャンネルが選択された後に検出器１２４で測定される。ここで、検出器１２４は、熱雑音、ショート雑音、電気雑音などの内部的な雑音だけでなく、他のチャンネルの信号によって発生する相互変調雑音などの影響を受ける。

【００２５】このとき、第１使用者装置のエンコーダ（または変調器）１０２を含む変調装置（図示せず）は、エンコーダ（または変調器）１０２をランダムビットシーケンス発生器（図示せず）に接続して、電気信号または光信号をランダムなビットシーケンスに変調させる。一方、第２使用者装置の復調装置（図示せず）は前記した過程を逆に行う。

【００２６】図２は、実際の暗号通信システムにおいて、秘密キーの共有時の暗号化及び暗号解除構造を説明するためのブロック図である。本発明による秘密キー同意方法により正規使用者間で秘密キー２６０を共有した後に、デジタル暗号システム（ＤＥＳ：Ｄｉｇｉｔａｌ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｙｓｔｅｍ）または３重ＤＥＳなどによるブロック暗号２７０を利用して、暗号化器２１０での暗号化関数の入力に秘密キー２６０を用いて、エンコーダ２００を通過した平文の内容を暗号化する。次に、同期デジタル伝送方式（ＳＤＨ：Ｓｙｎｃｒｏｎｏｕｓ　Ｄｉｇｉｔａｌ　Ｈｉｅｒａｒｃｈｙ）、ＣＤＭＡなどの伝送方式によるフレーマ２２０を利用してデータフレームを作成する。

【００２７】暗号解除は、この過程を逆に行う。伝送されてきた暗号データは、デフレーマ２３０を経て暗号解除器２４０に入力される。このとき、ブロック暗号２７０と秘密キー２６０とを用いて暗号が解除され、デコーダ２５０に渡される。

【００２８】図３は、光ＣＤＭＡ方式を利用した暗号通信システムにおいて、エンコーダ／デコーダの具現例を説明するための図面である。図３（ａ）は、時間遅延を内部的に生じる場合を、図３（ｂ）は、時間遅延を外部的に生じる場合を各々示している。

【００２９】図３（ａ）及び図３（ｂ）において、Ｎ対の使用者間の通信のために、Ｎ個のエンコーダが並列で接続されており、そこにマッチされるＮ個のデコーダが並列で接続されている。第１使用者装置の信号ソースで生じた信号はＣＤＭＡエンコーダ、フレーマを通過しつつ、ランダムなビットシーケンスに変調される。ここで、信号ソースは、各チャンネルが各々の光源をもっているか、多数個のチャンネルが一つの共有された信号ソースを分離したりスペクトル分割して用いる。

【００３０】その後、変調された信号は他の使用者装置内で生じた信号と共にマルチプレクサに入力され、共通の伝送媒体を用いて伝送される。伝送された信号はマルチプレクサによって分離されて受信端の使用者装置に供

給され、その使用者装置にマッチするデコーダを通じてフィルタリングされた後に検出される。

【００３１】各エンコーダは、不均衡のＭＺＩ（Ｍａｃｈ－Ｚｅｎｄｅｒ　Ｉｎｔｅｒｆｅｒｏｍｅｔｅｒ：マッハツェンダー干渉計）のように固有の時間遅延を招いたり、固有の周波数だけを通過／反射できるように、固有のコードに合わせて振幅または周波数を割当て可能にする装置であり、ここで、各エンコーダの固有の時間遅延は信号ソースの干渉時間よりも長くなければならない。

【００３２】各デコーダは、前記したエンコーダにマッチされる時間遅延またはコードミキサをもっていて、信号を他の信号と区別できる装置である。

【００３３】図４の（ａ）ないし（ｄ）は、時間遅延が生じるＣＭＤＡ方式の暗号通信システムにおいて、各地点でのパルス信号の時間的な変化を示した図である。図４（ａ）に示す信号ソースからの信号は、第１使用者装置のエンコーダとしての経路差のある干渉計の両アームを経て、図４（ｂ）のように時間遅延τ１をもつ二つのパルスに分離される。その後、第２使用者装置のデコーダを経て、４つのパルスに分離される。

【００３４】このとき、図４（ｃ）のように、エンコーダ及びデコーダの時間遅延差が一致する場合、中央に位置した２つのパルスが互いにコヒーレントに干渉を起こし、これにより信号がデコーディングされる。一方、図４（ｄ）のように、エンコーダ及びデコーダの時間遅延差が一致しない場合、中央に位置した２つのパルスは、パルス間に時間的な相関性がないため干渉を起こさず、検出器で検出できなくなる。

【００３５】本発明の基本的な動作原理は、第一に、雑音に敏感な比較的弱い強度の信号を伝送して、外部の攻撃者をして伝送された信号値を区別し難くすることである。第二に、外部の攻撃者をして正規使用者と互いに相関関係のない結果を取得させるために、背景雑音または測定器の雑音などのように相関関係のない雑音を用いることである。

【００３６】図５は、本発明によるキー同意方法を説明するためのフローチャートである。図５において、先ず、第１使用者装置で、信号ソースからの信号をエンコーダを用いて任意のビットシーケンスに変調して第２伝送装置に伝送する（ステップ５００）。第２使用者装置では、伝送された信号を受信して、第１使用者装置のエンコーダとマッチされたデコーダによってフィルタリングされた信号のビットの値を測定して記録する（ステップ５０２）。このとき、ステップ５００で伝送された信号は雑音に敏感な比較的弱い強度の信号であり、ステップ５０２で受信されたビットの測定値は、相互変調雑音、背景雑音または測定器の熱雑音により実際に伝送された信号を中心として分散・分布される。

【００３７】次に、第２使用者装置では、予め定められたしきい値以上の測定値をもつ、値が確実なビットだけをキーストリングとして採択し、しきい値未満に該当するビットを無視する（ステップ５０４）。次に、第２使用者装置は第１使用者装置に対して、キーとして採択されたビットの値の代わりに何番目のビットであるか、その番号だけを通知する（ステップ５０６）。第１使用者装置及び第２使用者装置は、それらの測定に基づいて、採択された所定番目のビットを秘密キーとして採択して共有し、残りのビットを捨てる（ステップ５０８）。

【００３８】ステップ５０８後に、第１使用者装置と第２使用者装置との間で共有されたキーストリングのうち任意の部分集合ビットを選択して、パリティチェックまたはエラーチェックを行い（ステップ５１０）、エラー率が許容値内に含まれるかどうかを判断する（ステップ５１２）。エラー率が許容値を超えた場合は、伝送に安全性が欠けて盗聴の危険性があるとみなして、採択されたビットの値を廃棄し、ステップ５００に戻って新しい伝送を行う。

【００３９】一方、エラー率が許容値内に含まれる場合は、その伝送は安全性が確保されているとみなす。この場合、エラー訂正やハッシュ関数を利用した増幅を行い、最適化されたキーストリングを得る（ステップ５１４）。そして前記した方法により共有したキーを秘密キーとして、通信信号の内容を暗号化或いは暗号解除を行う（ステップ５１６）。

【００４０】ここで、ステップ５００で雑音に敏感な比較的弱い強度の信号を伝送すれば、第２使用者装置における測定値にも多くのエラーを生じうる。これを補完するために、ステップ５０４からステップ５０８において、第２使用者装置が予め定められたしきい値以上の測定値をもつビットの信号だけをキーとして採択し、残りのビットを捨てることにより、第２使用者装置の測定値エラーが低減できる。

【００４１】一方、ステップ５００で伝送媒体を通じて信号が伝送される間に、盗聴者、すなわち、外部の攻撃者が侵入することがある。盗聴者が伝送信号を測定する場合、このときにも相互変調雑音または盗聴者が使用する装置の熱雑音により、測定値は実際に伝送された信号を中心として分散・分布される。しかし、正規使用者及び盗聴者は互いに独立的な装置を使用し、これにより、測定される結果に影響を及ぼす雑音も互いに相関関係無しに独立的に作用する。従って、盗聴者装置の雑音が第２使用者装置と相関関係無しに独立的に作用するため、盗聴者装置の測定値は第２使用者装置の測定値に関係無い異なる値をもちうる。

【００４２】しかも、伝送されるビットシーケンスの何番目のビットの値がキーとして採択されるかが分からないため、全ての測定値、すなわち、予め定められたしきい値以下の測定値をもつビットの測定結果も用いることになり、正規使用者よりも格段に多いエラーを含むキー

ストリングが得られることになる。また、盗聴者装置では、しきい値を超えない、値が確実でないビットを含む全てのビットに対して測定しなければならないので、エラー率が高くなる。

【００４３】このように、盗聴者が侵入に成功しなかった場合、盗聴者は第２使用者との相関関係を高めるために、第２使用者装置に測定値を再伝送することができる。盗聴者装置での高いエラー率の伝播により、第２使用者装置での測定値上に期待値よりも高いエラー率が生じる。従って、ステップ５１０のようにエラーチェックを行った場合、盗聴の有無が分かる。

【００４４】例えば、図２において、支配的な雑音要素は、好ましくない他の使用者装置（送信装置）からの信号が第２使用者装置にビーティングを起こして生じる相互変調雑音である。マッチされてない使用者装置（送信装置）からの相互干渉を考慮して本発明によるキー同意方法を適用した場合、盗聴者装置のキーストリングでの＊エラー率は、下記式（１）のように表わせる。

【００４５】

【数１】

$$P_e^E \approx \frac{1}{2} erfc\left(\frac{1}{\sqrt{4N^2 \cdot RIN \cdot B_R}}\right) \quad \cdots (1)$$

【００４６】ここで、Ｎは多重アクセスする使用者対の数であり、ＲＩＮは相対的な雑音強度であり、B_Rは受信装置の帯域幅である。第２使用者装置側でしきい値をθと定め、それ以上の測定値だけをキーとして採択したと仮定する。このとき、相互変調雑音により第２使用者装置のキーストリングに生じたエラー率は、盗聴者がない正常状態の場合には下記式（２－１）のように、盗聴者が侵入して盗聴した後に測定値を再伝送した場合には下記式（２－２）のように表わせる。

【００４７】

【数２】

$$P^B \approx \frac{1}{2} erfc\left(\frac{\theta/\sqrt{E}+1}{\sqrt{4N^2 \cdot RIN \cdot B_R}}\right) \quad \cdots (2-1)$$

$$\overline{P}_e^B \approx \frac{1}{4} erfc\left(\frac{1}{2\sqrt{RIN \cdot B_R}}\right) erfc\left(\frac{\theta/\sqrt{E}-1}{2\sqrt{RIN \cdot B_R}}\right) + \frac{1}{2}\left\{1-\frac{1}{2} erfc\left(\frac{1}{2\sqrt{RIN \cdot B_R}}\right)\right\} erfc\left(\frac{\theta/\sqrt{E}+1}{2\sqrt{RIN \cdot B_R}}\right) \quad \cdots (2-2)$$

【００４８】ここで、Ｅは伝送信号の振幅を表わす。例えば、４対の使用者が通信する場合、ＲＩＮ＝－１００ｄＢ／Ｈｚであり、$\theta = 3E^{1/2}$であれば、第２使用者装置のキーストリングのエラー率は０．０２５であるのに対し、盗聴者装置のキーストリングのエラー率は０．２６となる。また、相関関係を高めるために、盗聴者装置が自分の測定結果に基づき測定値を再伝送すれば、第２使用者装置のキーストリングのエラー率は約０．１７ほどに高くなるので、このエラー率の変化値がデータの汚染度を表わすことになり、これにより、盗聴の発生可否が分かるようになる。

【００４９】ここで、しきい値を高く設定するほど安全性は高くなるが、多くのビットを捨てる必要があるため、その分伝送速度が遅くなる。すなわち、データの伝送速度は下記式（３）のように表わせる。

【００５０】

【数３】

$$R \approx N \cdot \frac{1}{2} erfc\left(\frac{\theta/\sqrt{E}-1}{2\sqrt{RIN \cdot B_R}}\right) \quad \cdots (3)$$

【００５１】許容エラー率を０．０２５としたとき、２対の使用者の場合には、許容エラー率を満足するためのしきい値は$\theta = E^{1/2}$であるのに対し、４対の使用者の場合には、許容エラー率を満足するためのしきい値は約３倍高く設定する必要がある。その結果、データの伝送速度は約６２％に減少することになる。従って、安全性及び多くの使用者の受容のために高いしきい値が要求され、これは、伝送速度を制限する要因となりうる。

【００５２】図６は、本発明によるキー同意方法を光ＣＤＭＡ方式に適用した場合に採択されたキーストリングでのエラー率を示した図である。ここで、点線は盗聴汚染があるときの受信側の使用者装置の場合$\theta = E^{1/2}$と定めたときを、実線は盗聴者装置の場合$\theta = 3E^{1/2}$と定めたときをそれぞれ表わす。使用者の数が定まると、一定の許容エラー率を満足するためのしきい値を導き出せる。安全性のためには高いしきい値が要求されるが、データ伝送速度及びトレードオフを考慮して定めることができる。

【００５３】

【発明の効果】以上述べたように、本発明は、物理的な階層で安全性を構築するので、従来のアルゴリズムを利用した方式とは異なって、複雑な数学計算を必要とせず、これにより、後段階の信号処理も簡単である。また、アルゴリズムを利用した方式の脆弱性が排除され、信号処理の前段階である伝送段階に適用する場合、秘密キーを使用してブロック単位の信号に安全機能を与える方式に、ブロック暗号の安全性を一層強化することができる。

【００５４】また、本発明は、盗聴者や不正使用者が正規使用者と同一のキーを入手できないだけでなく、通信システムでの盗聴の発生可否及びその度合いを推測することができる。盗聴者が測定値を再伝送した時の受信データで生じたエラーを検出し、実験的な環境で期待されるエラー率と比較することにより、その受信データが盗

聴によりどれくらい汚染されたかが検出できる。正規使用者と盗聴者との間の観測値に互いに相関関係がないように誘導するという基本原理は、光通信だけでなく、従来の有線通信や無線通信にそのまま適用できるので、その基本原理の応用範囲は無限である。

【００５５】また、本発明は、いかなる通信システム上の雑音も利用可能なので、適用可能な通信システムは無限である。高品質及び高水準の装置の開発を前提とせず、設置が容易であるほか、従来の装置のほかに付加装置が不要であり、即座に適用可能である。従って、別のチャンネルを用いることなしに、一般的な通信システムを一時的に秘密キーの伝達チャンネルとして活用した後、安全モード時に共通キーを暗号化して通信を行うことができる。

【００５６】特に、ＣＤＭＡ方式を利用した場合には、多数の使用者がタイミングを同期化する必要なしに、同時に全ての周波数帯域を共用したまま非同期伝送を行う。このとき、安全性及び安定性が向上されて、一般的な通信システムをそのままキー同意だけでなく、暗号文を伝送するセキュア通信システムとして利用できる。双方向通信及び容易にアドレス交換が可能な実用的な通信システムを構築できる。

【００５７】また、本発明は、信号の増幅が不可能な量子暗号に対して信号増幅が可能なので、ＬＡＮ環境で多重アクセス方式への適用のみならず、ＷＡＮ環境でも多重アクセス方式への適用が可能である。

【図面の簡単な説明】

【図１】本発明が適用される一般的な通信システムにおける通信チャンネルの構造を説明するためのブロック図である。

【図２】実際の暗号通信システムにおいて、秘密キーの共有時における暗号化及び暗号解除の構造を説明するためのブロック図である。

【図３】光ＣＤＭＡ方式を利用した暗号通信システムにおいて、エンコーダ／デコーダの具現例を説明するための図であり、（ａ）は時間遅延を内部的に生じる場合、（ｂ）は時間遅延を外部的に生じる場合を示す。

【図４】時間遅延されたＣＤＭＡ方式の暗号通信システムにおいて、各地点でのパルス信号の時間的な変化を示した図であり、（ａ）は信号ソースからの信号、（ｂ）はエンコーダの結果、（ｃ）はマッチされたデコーダの結果、（ｄ）はマッチされていないデコーダの結果を示す。

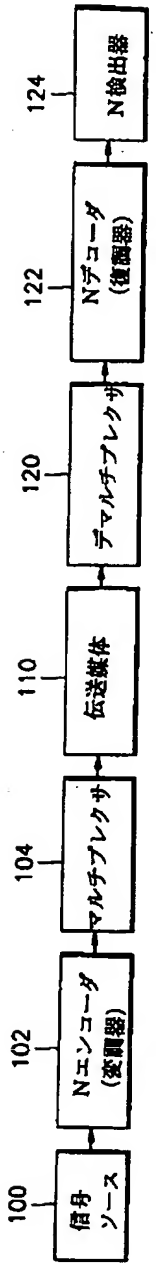
【図５】本発明によるキー同意方法を説明するためのフローチャートである。

【図６】本発明によるキー同意方法を光ＣＤＭＡ方式に適用した場合に採択されたキーストリングでのエラー率を示した図である。

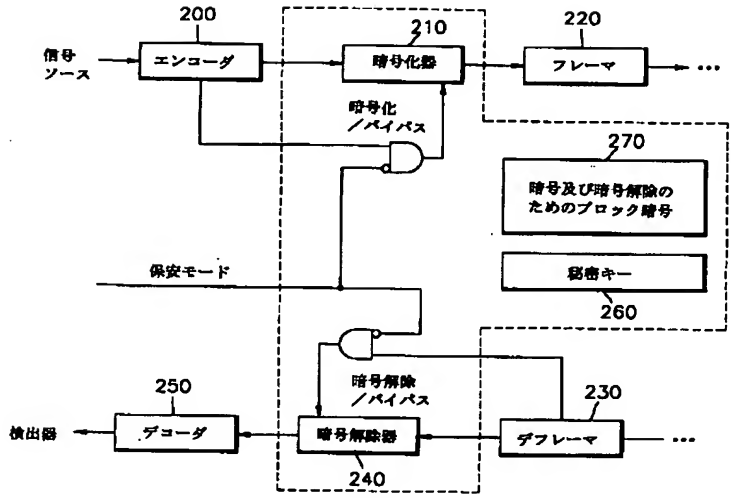
【符号の説明】

１００　信号ソース
１０２　エンコーダ（変調器）
１０４　マルチプレクサ
１１０　伝送媒体
１２０　デマルチプレクサ
１２２　デコーダ（復調器）
１２４　検出器
２００　エンコーダ
２１０　暗号化器
２２０　フレーマ
２３０　デフレーマ
２４０　暗号解除器
２５０　デコーダ
２６０　秘密キー
２７０　暗号及び暗号解除のためのブロック暗号

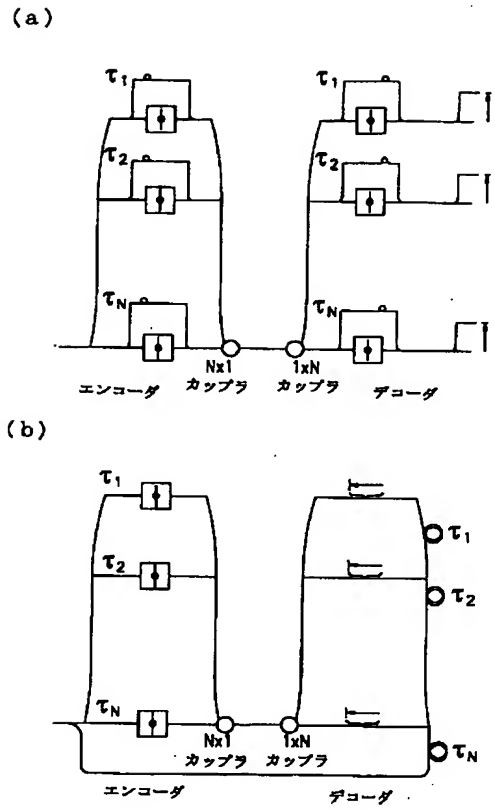
【図１】


100
信号ソース
102
Nエンコーダ（変調器）
104
マルチプレクサ
110
伝送媒体
120
デマルチプレクサ
122
Nデコーダ（復調器）
124
N検出器

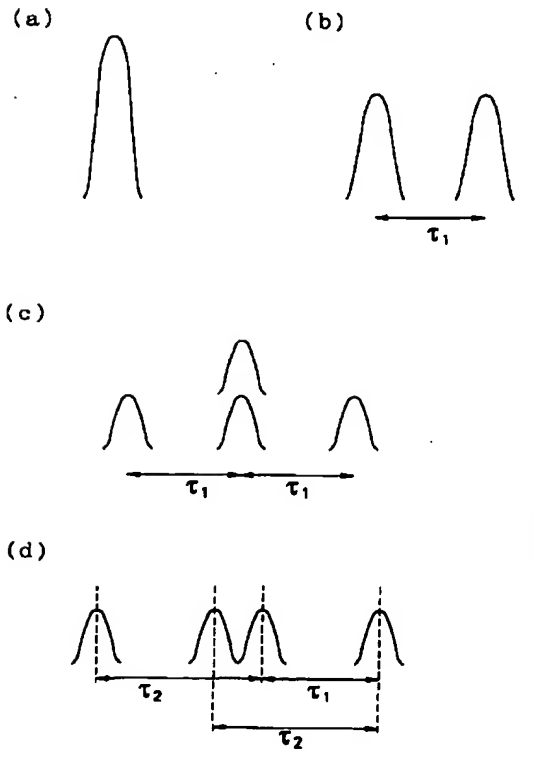
【図２】


200
210
220
信号ソース
エンコーダ
暗号化器
フレーマ
暗号化／バイパス
270
暗号及び暗号解除のためのブロック暗号
保安モード
秘密キー
260
250
230
検出器
デコーダ
暗号解除器
デフレーマ
暗号解除／バイパス
240

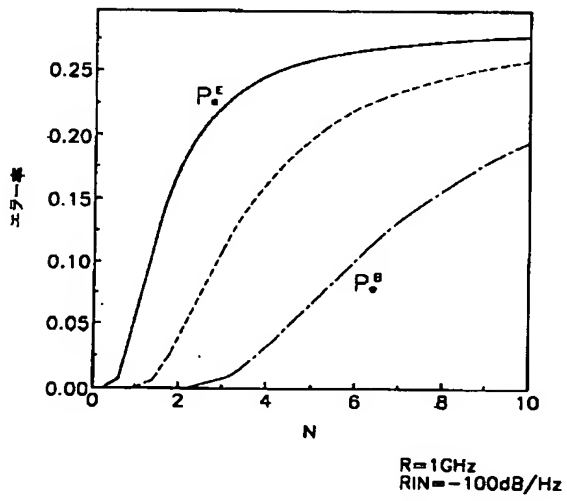
【図３】


(a)
τ_1
τ_2
τ_N
Nx1 カップラ
1xN カップラ
エンコーダ
デコーダ
(b)

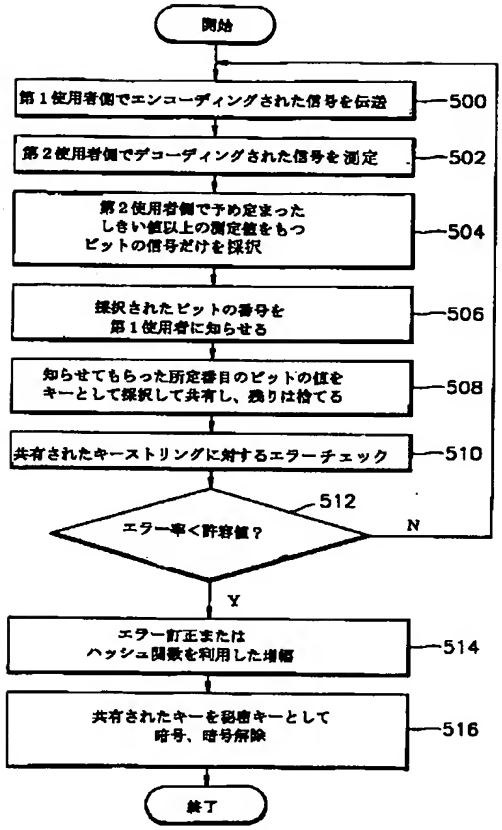
【図４】


(a)
(b)
τ_1
(c)
τ_1 τ_1
(d)
τ_2 τ_1
τ_2

【図６】


0.25
0.20
0.15
0.10
0.05
0.00
0
2
4
6
8
10
N
R=1GHz
RIN=−100dB/Hz

【図５】


開始
第１使用者側でエンコーディングされた信号を伝送
500
第２使用者側でデコーディングされた信号を測定
502
第２使用者側で予め定まった
しきい値以上の測定値をもつ
ビットの信号だけを採択
504
採択されたビットの番号を
第１使用者に知らせる
506
知らせてもらった所定番目のビットの値を
キーとして採択して共有し、残りは捨てる
508
共有されたキーストリングに対するエラーチェック
510
512
エラー率く許容値？
N
Y
エラー訂正または
ハッシュ関数を利用した増幅
514
共有されたキーを秘密キーとして
暗号、暗号解除
516
終了